National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DNS-BASED SECURE EMAIL

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenge of Domain Name System (DNS) based secure email through collaborative efforts with members of the information technology (IT) community, including vendors of cybersecurity solutions. This sheet provides an overview of the background and challenge, goals, and proposed solution. For more information about the project, see the white paper, *DNS-Based Security for Electronic Mail* on the NCCoE website. We also believe that our proposed solution may not be the only one available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or learn about products that might be applicable to the challenge of DNS-based email security, please contact us at dns-email-nccoe@nist.gov.

BACKGROUND

Both public and private sector business operations rely on email exchanges. The need to protect business plans and strategies; the integrity of transactions, financial, and other proprietary information; and privacy of employees and clients are only some of the factors that motivate organizations to secure their email exchanges. Whether the security service desired is authentication of the source of an email message, assurance that the message has not been altered by an unauthorized party, or confidentiality of message contents, cryptographic functions are usually employed in providing the service. But many current server-based email security mechanisms are vulnerable to and have been defeated by attacks on the integrity of the cryptographic implementations on which they depend.

THE CHALLENGE

Organizations need to protect their server-based email security mechanisms against intrusion and man-in-the-middle attacks during the automated cryptographic service negotiation process. In the absence of appropriate combination protections, any of these attacks can result in reading or modification of information by unauthorized third parties. The attacks can also enable an attacker to pose as one of the parties to an email exchange and send email that contains links to malware-ridden websites. If other content in a fraudulent message successfully motivates the user to click on the link or the user's system is configured to automatically follow some links or download content other than text, the malware will infect the user's system. Inclusion of links to malware is a major factor in most confirmed data breaches. Consequences of such breaches can range from exposure of sensitive or private information to enabling fraudulent activity by the attacker posing as the victimized user and disabling or destroying the user's system—or that of the user's parent organization.

GOALS

The DNS-based secure email project will demonstrate a security platform that provides trustworthy mail server-to-mail server email exchanges across organizational boundaries. To address real-world business challenges related to secure email exchanges, the NCCoE is developing an example solution composed of open-source and commercially available components.

The goal of the secure email project is to provide tools that help organizations:

- encrypt email traffic between servers
- allow individual email users to digitally sign and/or encrypt email messages to other end users
- allow individual email users to obtain other users' certificates in order to validate signed email or send encrypted email
- generate information that can be queried by email recipients to identify valid email senders for a domain and that a given message originated from one of the valid senders

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
dns-email-nccoe@nist.gov
301-975-0200

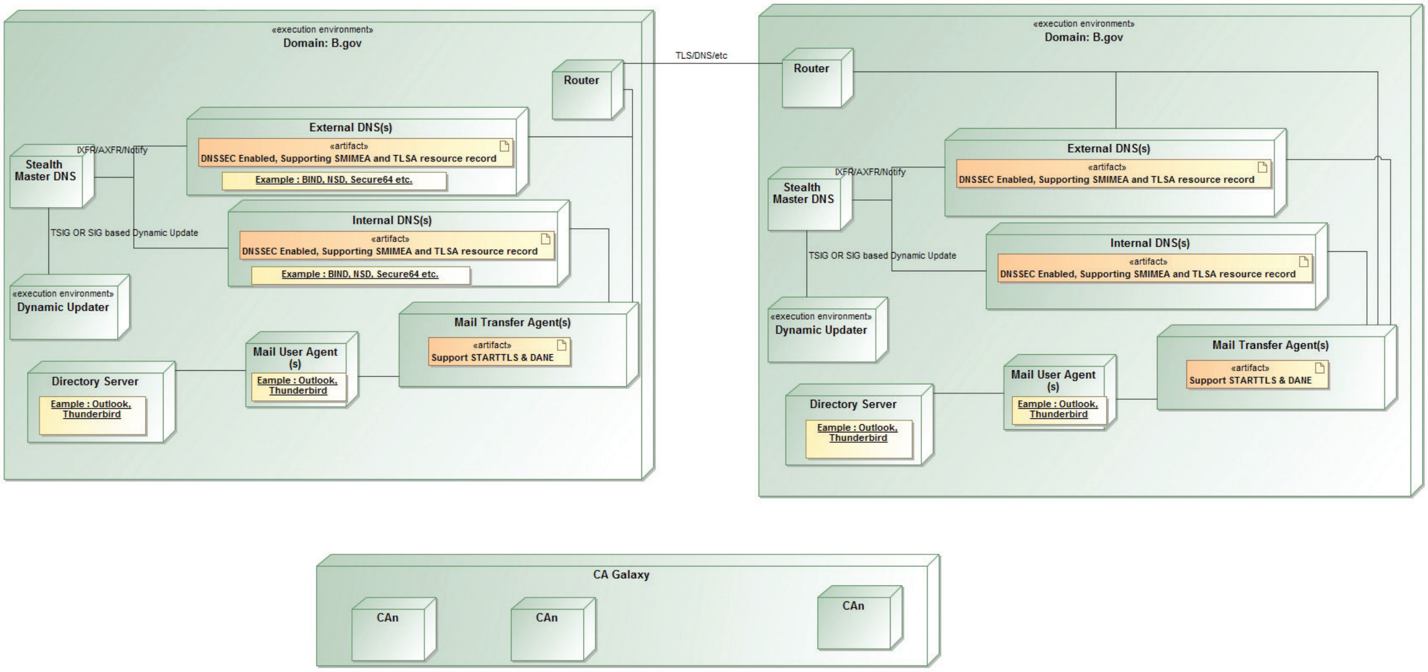
BENEFITS

The business value of the security platform that results from the secure email project will include:

- improved privacy and security protections for users' operations
- expansion of the set of DNS security applications
- increased confidence that entities to which users believe they are connecting are the entities to which they are actually connecting

ARCHITECTURE

In both scenarios in this example architecture, encryption is performed by the email servers on bulk exchanges between email services. This addresses the main security concerns in enterprise environments, which are the target of the project, but not necessarily those of individual users who may also want to reduce information disclosure to their email providers. The only per-message cryptography is digital signatures. In the second scenario, digital signature protection is provided by the clients.



HOW TO PARTICIPATE

As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you are interested in contributing or collaborating on this project to enhance DNS-based secure email exchanges, please contact us at dns-email-nccoe@nist.gov.

For more information about this project, visit: https://nccoe.nist.gov/projects/building_blocks/secured_email